PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of

Hong-young JEON, et al.

Docket No: Q101767

Appln. No.: **11/829,421**

Group Art Unit: Unknown

Confirmation No.: **1126**

Examiner: Not Yet Assigned

Filed: July 26, 2007

For: METHOD AND APPARATUS FOR DIGITAL RIGHTS MANAGEMENT

SUBMISSION OF PRIORITY DOCUMENT

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Submitted herewith is a certified copy of the priority document on which a claim to priority was made under 35 U.S.C. § 119. The Examiner is respectfully requested to acknowledge receipt of said priority document.

Respectfully submitted,

/darrylmexic/

Darryl Mexic
Registration No. 23,063

SUGHRUE MION, PLLC
Telephone: (202) 293-7060
Facsimile: (202) 293-7860

WASHINGTON OFFICE
23373
CUSTOMER NUMBER

Enclosures: Korea, Republic of 10-2006-0106835

Date: July 27, 2007

Issue Number : 5-5-2007-018189152

대한민국특허청
KOREAN INTELLECTUAL PROPERTY OFFICE

별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto is a true copy from the records of the Korean Intellectual Property Office.

출원번호 : Application Number		10-2006-0106835
출원년월일 : Filing Date		2006년 10월 31일 OCT 31, 2006
출원인 : Applicant(s)		삼성전자주식회사 SAMSUNG ELECTRONICS CO., LTD.

2007년 04월 06일

특허청 COMMISSIONER

◆ This certificate was issued by Korean Intellectual Property Office. Please confirm any forgery or alteration of the contents by an issue number or a barcode of the document below through the KIPOnet- Online Issue of the Certificates' menu of Korean Intellectual Property Office homepage (www.kipo.go.kr). But please notice that the confirmation by the issue number is available only for 90 days.

【서지사항】

【서류명】	특허출원서
【권리구분】	특허
【수신처】	특허청장
【제출일자】	2006.10.31
【발명의 국문명칭】	디지털 저작권 관리 방법 및 장치
【발명의 영문명칭】	Method and apparatus for digital rights management
【출원인】	
【명칭】	삼성전자 주식회사
【출원인코드】	1-1998-104271-3
【대리인】	
【성명】	김동진
【대리인코드】	9-1999-000041-4
【포괄위임등록번호】	2002-007585-8
【대리인】	
【성명】	정상빈
【대리인코드】	9-1998-000541-1
【포괄위임등록번호】	2003-003437-4
【발명자】	
【성명】	전홍영
【성명의 영문표기】	JEON, Hong Young
【주민등록번호】	811121-2XXXXXXX
【우편번호】	441-390
【주소】	경기 수원시 권선구 권선동 세종 그랑시아 오피스텔 227호
【국적】	KR
【발명자】	
【성명】	정명준
【성명의 영문표기】	JUNG, Myung June

【주민등록번호】 741130-1XXXXXXX

【우편번호】 443-740

【주소】 경기 수원시 영통구 영통동 황골마을1단지아파트 156동 1103호

【국적】 KR

【발명자】

【성명】 최현진

【성명의 영문표기】 CHOI, Hyun Jin

【주민등록번호】 700329-1XXXXXXX

【우편번호】 135-935

【주소】 서울 강남구 역삼1동 827-55 스마일빌라 101호

【국적】 KR

【발명자】

【성명】 정경임

【성명의 영문표기】 JUNG, Kyung Im

【주민등록번호】 720801-2XXXXXXX

【우편번호】 463-728

【주소】 경기 성남시 분당구 수내동 파크타운롯데아파트 128동 903호

【국적】 KR

【발명자】

【성명】 김지수

【성명의 영문표기】 KIM, Ji Soo

【주민등록번호】 740515-1XXXXXXX

【우편번호】 448-750

【주소】 경기 용인시 수지구 상현동 풍산아파트 102동 701호

【국적】 KR

【발명자】

【성명】 이선재

【성명의 영문표기】 LEE, Sun Jae

【주민등록번호】 790203-1XXXXXXX

【우편번호】 443-813

【주소】 경기 수원시 영통구 영통동 1042-4번지 301호

【국적】 KR

【발명자】

【성명】 심억수

【성명의 영문표기】 SHIM, Eok Soo

【주민등록번호】 800115-1XXXXXXX

【우편번호】 443-370

【주소】 경기 수원시 영통구 매탄동 802-3

【국적】 KR

【심사청구】 청구

【취지】 특허법 제42조의 규정에 의한 출원, 특허법 제60조의 규정에 의한 심사청구를 합니다.

대리인 김동진 (인)

대리인 정상빈 (인)

【수수료】

【기본출원료】	0 면	38,000 원
【가산출원료】	49 면	0 원
【우선권주장료】	0 건	0 원
【심사청구료】	45 항	1,549,000 원
【합계】	1,587,000 원	

【요약서】

【요약】

본 발명은 디지털 저작권 관리 방법 및 장치에 관한 것이다.

본 발명의 실시예에 따른 디지털 저작권 관리 방법은, 컨텐츠에 대한 재생 권한을 갖는 메인 디바이스로부터 상기 컨텐츠의 사용을 허가한다는 정보를 포함하는 증명서를 발급 받는 단계, 상기 증명서를 서비스 제공 장치에게 전송하는 단계, 및 상기 서비스 제공 장치로부터 상기 컨텐츠를 제공 받는 단계를 포함한다.

【대표도】

도 1

【색인어】

디지털 저작권 관리, 컨텐츠, 권리 객체, 증명서

【명세서】

【발명의 명칭】

디지털 저작권 관리 방법 및 장치{Method and apparatus for digital rights management}

【도면의 간단한 설명】

<1> 도 1은 본 발명의 일 실시예에 따른 DRM 시스템을 나타낸 도면이다.

<2> 도 2는 본 발명의 일 실시예에 따른 상호 인증 과정을 나타낸 흐름도이다.

<3> 도 3은 본 발명의 일 실시예에 따른 원격 디바이스가 메인 디바이스로부터 증명서를 발급 받는 과정을 나타낸 흐름도이다.

<4> 도 4는 본 발명의 일 실시예에 따른 원격 디바이스의 컨텐츠 재생 과정을 나타낸 흐름도이다.

<5> 도 5는 본 발명의 일 실시예에 따른 메인 디바이스를 나타낸 블록도이다.

<6> 도 6은 본 발명의 일 실시예에 따른 원격 디바이스를 나타낸 블록도이다.

<7> 도 7은 본 발명의 일 실시예에 따른 서비스 제공 장치를 나타낸 블록도이다.

<8> <도면의 주요 부분에 관한 부호의 설명>

<9> 110 : 메인 디바이스 120 : 원격 디바이스

<10> 130 : 서비스 제공 장치 140 : 컨텐츠 공급 서버

【발명의 상세한 설명】

【발명의 목적】

【발명이 속하는 기술분야 및 그 분야의 종래기술】

<11> 본 발명은 디지털 저작권 관리에 관한 것으로서, 더욱 상세하게는 디지털 저작권 관리 방법 및 장치에 관한 것이다.

<12> 최근에 디지털 저작권 관리(Digital Rights Management; 이하, "DRM"이라 함)에 관한 연구가 활발하며, DRM을 적용한 상용 서비스들이 도입되었거나 도입 중에 있다. DRM은 무단 복제 및 배포가 용이한 디지털 컨텐츠를 보호하기 위한 기술 개념이다.

<13> 디지털 컨텐츠를 보호하고자 하는 노력은 종래에도 있었으나, 종래의 기술은 디지털 컨텐츠에 대한 무단 접근 방지에 중점을 두고 있었다. 예컨대 디지털 컨텐츠에 대한 접근(access)은 대가를 지불한 사용자에게만 허용되었으며, 대가를 지불하지 않은 사용자는 디지털 컨텐츠에 접근할 수 없었다. 그러나 디지털 데이터의 특성상 디지털 컨텐츠는 재사용, 가공, 복제 및 배포가 용이하다. 따라서 대가를 지불하고 디지털 컨텐츠에 접근한 사용자가 이를 무단으로 복제 또는 배포할 경우에는 대가를 지불하지 않은 사용자도 디지털 컨텐츠를 사용할 수 있게 된다.

<14> 이러한 문제점을 보완하기 위해 DRM은 디지털 컨텐츠를 암호화하여 배포하도록 하고, 암호화된 디지털 컨텐츠를 사용하기 위해서는 권리 객체(Rights Object; RO)라는 라이센스가 필요하도록 한다. 따라서 컨텐츠를 사용하려는 디바이스는 반드시 권리 객체를 저장하여야 하거나, 권리 객체를 저장하고 있는 다른 디바이스와 통신이 가능해야 한다. 또한, 권리 객체가 컨텐츠와 일체화되어 존재한다면, 컨텐

츠를 저장하고 있는 디바이스 이외의 다른 디바이스를 통해서는 해당 컨텐츠를 이용할 수 없게 된다. 물론, 컨텐츠나 권리 객체가 디바이스 간에 복사되거나 이동될 수도 있지만, 복사나 이동에는 일정한 제한(예를 들어 임계 횟수 이상 이동이 금지될 수 있다)이 따른다.

<15> 한국공개특허 10-2005-0045883(컨텐츠 공유 시스템, 컨텐츠 처리 장치, 정보 처리 장치, 프로그램, 기록 매체, 및 컨텐츠 공유 방법)에는 컨텐츠를 제공하는 디바이스를 특정하는 소스 ID를 컨텐츠에 부가하고, 컨텐츠를 취득하는 디바이스는 커텐츠에 부가된 소스 ID를 포함하는 재생 허가 ID 리스트를 구비함으로서, 디지털 저작권을 보호하면서도 디바이스 간에 컨텐츠를 공유할 수 있는 기술을 개시하고 있다. 그러나, 한국공개특허 10-2005-0045883에 의할 경우, 컨텐츠 공유를 위해서는 디바이스 간에 컨텐츠가 직접 전달되어야 한다. 따라서, 컨텐츠를 수신할 디바이스의 저장 능력에 따라서 컨텐츠의 이동 가능성이 제한될 수 있으며, 서로 통신할 수 없는 상태에 있는 디바이스 간에는 컨텐츠를 공유할 수 없는 문제점이 있다.

<16> 따라서 디지털 저작권을 안전하게 보호하면서, 컨텐츠를 구입한 사용자가 디바이스에 제한되지 않고 보다 유연하게 컨텐츠를 이용할 수 있도록 하기 위한 디지털 저작권 관리 기술이 요구되고 있다.

【발명이 이루고자 하는 기술적 과제】

<17> 본 발명은 디지털 저작권 관리로 보호되는 컨텐츠를 보다 유연하게 사용할 수 있도록 하는데 그 목적이 있다.

<18> 본 발명의 목적들은 이상에서 언급한 목적들로 제한되지 않으며, 언급되지 않은 또 다른 목적들은 아래의 기재로부터 당업자에게 명확하게 이해될 수 있을 것이다.

【발명의 구성】

<19> 상기 목적을 달성하기 위하여, 본 발명의 실시예에 따른 디지털 저작권 관리 방법은, 컨텐츠에 대한 재생 권한을 갖는 메인 디바이스로부터 상기 컨텐츠의 사용을 허가한다는 정보를 포함하는 증명서를 발급 받는 단계, 상기 증명서를 서비스 제공 장치에게 전송하는 단계, 및 상기 서비스 제공 장치로부터 상기 컨텐츠를 제공 받는 단계를 포함한다.

<20> 상기 목적을 달성하기 위하여, 본 발명의 실시예에 따른 디지털 저작권 관리 방법은, 컨텐츠의 사용을 허가한다는 정보를 포함하는 증명서를 원격 디바이스에게 발급하는 단계, 상기 원격 디바이스에게 상기 컨텐츠를 제공하려는 서비스 제공 장치로부터 상기 컨텐츠를 재생시킬 수 있는 권리 객체의 상태 정보를 갱신할 것을 요청 받는 단계, 및 상기 상태 정보를 갱신하는 단계를 포함한다.

<21> 상기 목적을 달성하기 위하여, 본 발명의 실시예에 따른 디지털 저작권 관리 방법은, 원격 디바이스로부터 증명서 및 컨텐츠 전송 요청을 수신하는 단계, 상기 증명서가 메인 디바이스에 의해 발급되었는지의 여부를 검증하는 단계, 및 상기 증명서가 상기 메인 디바이스에 의해 발급된 것일 경우, 상기 컨텐츠를 상기 원격 디바이스에게 제공하는 단계를 포함한다.

<22> 상기 목적을 달성하기 위하여, 본 발명의 실시예에 따른 원격 디바이스는, 컨텐츠에 대한 재생 권한을 갖는 메인 디바이스로부터 상기 컨텐츠의 사용을 허가한다는 정보를 포함하는 증명서를 이용하여 서비스 제공 장치에게 상기 컨텐츠를 요청하는 요청부, 및 상기 서비스 제공 장치로부터 제공되는 상기 컨텐츠를 재생하는 재생부를 포함한다.

<23> 상기 목적을 달성하기 위하여, 본 발명의 실시예에 따른 메인 디바이스는, 상기 컨텐츠의 사용을 허가한다는 정보를 포함하는 증명서 생성하는 증명서 생성부, 상기 생성된 증명서를 원격 디바이스에게 전송하는 통신부, 상기 원격 디바이스에게 상기 컨텐츠를 제공하려는 서비스 제공 장치로부터 상기 컨텐츠를 재생시킬 수 있는 권리 객체의 상태 정보를 갱신하도록 요청 받은 경우, 상기 상태 정보를 갱신하는 제어부를 포함한다.

<24> 상기 목적을 달성하기 위하여, 본 발명의 실시예에 따른 서비스 제공 장치는, 원격 디바이스로부터 증명서 및 컨텐츠 전송 요청이 수신되는 경우, 상기 증명서가 메인 디바이스에 의해 발급되었는지의 여부를 검증하는 증명서 검증부, 및 상기 증명서가 상기 메인 디바이스에 의해 발급된 것일 경우, 상기 컨텐츠를 상기 원격 디바이스에게 제공하는 컨텐츠 제공부를 포함한다.

<25> 기타 실시예들의 구체적인 사항들은 상세한 설명 및 도면들에 포함되어 있다.

<26> 본 발명의 이점 및 특징, 그리고 그것들을 달성하는 방법은 첨부되는 도면과 함께 상세하게 후술되어 있는 실시예들을 참조하면 명확해질 것이다. 그러나 본

발명은 이하에서 개시되는 실시예들에 한정되는 것이 아니라 서로 다른 다양한 형태로 구현될 수 있으며, 단지 본 실시예들은 본 발명의 개시가 완전하도록 하고, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 발명의 범주를 완전하게 알려주기 위해 제공되는 것이며, 본 발명은 청구항의 범주에 의해 정의될 뿐이다. 명세서 전체에 걸쳐 동일 참조 부호는 동일 구성 요소를 지칭한다.

<27> 이하, 첨부된 도면을 참조하여 본 발명의 바람직한 실시예를 상세히 설명하기로 한다.

<28> 먼저 본 발명에서 사용되는 용어에 대하여 설명하도록 한다. 용어의 설명은 본 발명의 이해를 돕기 위한 것이다. 따라서 본 발명의 상세한 설명에 있어서 명시적으로 한정하지 않는 한, 이하 설명되는 용어들이 본 발명의 기술적 사상을 한정하는 의미로 사용되는 것이 아님에 주의해야 한다.

<29> - 컨텐츠

<30> 컨텐츠는 디지털 멀티디미어 데이터로서, 동영상, 정지영상, 오디오, 게임, 텍스트 등 그 종류에 제한되지 않는다. 바람직하게는 컨텐츠는 암호화된 상태로 존재할 수 있다.

<31> - 권리 객체 (Rights Object; RO)

<32> 권리 객체는 컨텐츠에 대한 사용 권한을 갖는 일종의 라이센스이다. 권리 객체는 컨텐츠 암호화 키, 제한 정보, 및 컨텐츠 식별자를 포함한다. 여기서, 컨텐츠 식별자는 컨텐츠 암호화 키로 재생(play back)시킬 수 있는 컨텐츠를 식별하

는데 사용되는 정보이다. 컨텐츠의 재생 방식의 예로써 플레이(play), 디스플레이(display), 실행(execute), 인쇄(print) 등을 들 수 있으며, 컨텐츠의 유형에 따라서 재생 방식도 달라질 수 있다. 예를 들어 컨텐츠가 동영상이나 음악에 관한 것이라면 재생 방식은 플레이일 수 있으며, 컨텐츠가 정지 영상에 관한 것이라면 재생 방식은 디스플레이나 인쇄일 수 있다. 또한 컨텐츠가 자바 게임에 관한 것이라면 재생 방식은 실행일 수 있다.

<33> 한편, 권리 객체는 컨텐츠와 독립된 별개의 개체일 수도 있고, 컨텐츠에 일체화되어 있을 수도 있다. 권리 객체에 포함되는 다른 정보들에 대해서는 이하에서 별도로 설명할 것이다.

<34> - 컨텐츠 암호화 키

<35> 컨텐츠 암호화 키는 컨텐츠를 재생(play back)시킬 수 있는 키이며 소정의 바이너리(binary) 값의 형태를 가질 수 있다. 예를 들어 컨텐츠 암호화 키는 암호화된 컨텐츠를 복호화하는데 사용될 수 있다.

<36> - 제한 정보(constraint information)

<37> 제한 정보는 컨텐츠를 재생시킬 수 있는 한도를 나타내는 정보로써, 하나의 권리 객체 내에는 하나 이상의 제한 정보가 설정될 수 있다. 제한 정보의 예로써 횟수(count) 제한, 일시(datetime) 제한, 기간(interval) 제한, 누적시간(accumulated) 제한 등을 들 수 있다.

<38> 여기서 횟수 제한은 컨텐츠를 재생시킬 수 있는 횟수를 한정한다. 예컨대

권리 객체에 횟수 제한이10으로 설정되어 있다면, 디바이스는 권리 객체를 소비하여 컨텐츠를 10번 재생시킬 수 있게 된다.

<39> 일시 제한은 컨텐츠를 재생시킬 수 있는 일시를 한정하며, 시작(start) 요소와 끝(end) 요소 중에서 적어도 하나를 포함할 수 있다. 디바이스는 일시 제한이 설정된 권리 객체를 소비할 경우, 일시 제한의 시작 요소가 지시하는 일시 이후에 컨텐츠를 재생시킬 수 있으며, 끝 요소가 지시하는 일시 이전까지 컨텐츠를 재생시킬 수 있게 된다. 예를 들어 권리 객체에 일시 제한이 시작 요소로써 2006년 10월 1일 0시 0분 0초로 설정되어 있다면, 디바이스는 2006년 10월 1일 0시0분0초 이후부터 권리 객체를 소비하여 컨텐츠를 재생시킬 수 있게 된다.

<40> 기간 제한은 권리 객체를 소비하여 컨텐츠를 재생시킬 수 있는 기간을 한정한다. 기간의 시작은 디바이스가 권리 객체를 소비하여 컨텐츠를 처음 재생시킨 시점으로 설정될 수 있다. 예컨대 권리 객체에 제한 정보로써 기간 제한이 1주일로 설정된 경우, 디바이스가 2006년 10월 1일 0시 0분 0초에 권리 객체를 처음으로 소비하여 컨텐츠를 재생시켰다면, 디바이스는 2006년 10월 8일 0시 0분 0초까지 권리 객체를 소비하여 컨텐츠를 재생시킬 수 있게 된다.

<41> 누적시간 제한은 권리 객체를 소비하여 컨텐츠를 재생시킬 수 있는 시간의 총 합을 한정한다. 예컨대 권리 객체에 누적시간 제한이 10시간으로 설정되어 있다면, 디바이스는 권리 객체를 소비하여 총 10시간 동안 컨텐츠를 재생시킬 수 있게 된다. 이때 디바이스는 권리 객체를 소비하여 컨텐츠를 재생시킨 횟수나 날짜에 대한 제한은 받지 않는다.

<42> - 상태 정보

<43> 권리 객체의 소비 정도를 나타내는 정보이다. 예를 들어, 횟수 제한이 설정된 권리 객체에 대응하는 상태 정보는 컨텐츠 재생 횟수에 대한 정보를 포함할 수 있다. 이 경우, 디바이스가 권리 객체를 소비하여 컨텐츠를 재생시키면, 상태 정보의 컨텐츠 재생 횟수가 카운트된다. 만약 권리 객체의 횟수 제한이 10회로 설정되어 있고, 상기 권리 객체에 대응하는 상태 정보의 컨텐츠 재생 횟수가 10회까지 카운트되었다면, 디바이스는 컨텐츠를 재생시키기 위해서 상기 권리 객체를 더 이상 사용할 수 없게 된다. 상태 정보는 권리 객체에 포함되어 있을 수 있다. 물론 상태 정보는 권리 객체와는 독립된 개체로 존재할 수도 있는데, 이 경우에도 상태 정보는 권리 객체에 종속적으로 관리된다.

<44> 권리 객체가 반드시 대응되는 상태 정보를 가져야 하는 것은 아니다. 예를 들어, 일시 제한이 설정되어 있는 권리 객체는 이를 사용하는 디바이스가 현재의 시간 정보를 권리 객체의 일시 제한과 비교함으로서, 권리 객체가 사용 가능한지 판단할 수 있을 것이므로, 이러한 경우 상태 정보를 관리하지 않아도 무방하다.

<45> - 공개키 암호화(Public-key Cryptography)

<46> 비대칭 암호화라고도 하며, 데이터를 암호화하는데 사용되는 키와 데이터를 복호화하는데 사용되는 키가 서로 다른 키로 구성된다. 공개키 암호화 방식에서 키는 공개키와 개인키를 포함한다. 공개키는 비밀로 보관될 필요가 없으며 일반에게 손쉽게 공개될 수 있고, 개인키는 특정 디바이스 자신만이 알고 있어야 한다. 공개키 암호화 알고리즘의 예로는 Diffie-Hellman 방식, RSA(Rivest Shamir

Adleman) 방식, ElGamal 방식, 및 타원곡선(Elliptic Curve) 방식 등이 있다.

<47> - 대칭키 암호화(Symetric-key Criptography)

<48> 비밀키 암호화라고도 하며, 데이터를 암호화하는데 사용되는 키와 데이터를 복호화하는데 사용되는 키가 동일한 키로 구성된다. 이러한 대칭키 암호화의 예로는 DES(Data Encryption Standard) 방식이 가장 일반적으로 사용되고 있으며, 최근에는 AES(Advanced Encryption Standard) 방식을 채용한 어플리케이션이 증가하고 있다.

<49> - 난수

<50> 난수는 임의성을 갖는 숫자열, 문자열, 또는 이들의 조합을 의미한다.

<51> - 인증서

<52> 인증서는 특정 디바이스가 정당한 장치임을 확인할 수 있는 정보이다. 예를 들어 인증서는 특정 디바이스의 ID(식별자)와 공개키를 포함할 수 있다. 또한, 인증서는 소정의 인증기관(Certification Authority)에 의해 발행되며 인증기관에 의해 전자서명 되어 있다. 디바이스는 통신하려는 상대 디바이스의 인증서를 통해서 상대 디바이스가 정당한 장치인지 확인할 수 있다.

<53> - 증명서

<54> 증명서는 디바이스가 자신이 보유하고 있는 컨텐츠의 재생 권한의 일부 또는 전부를 다른 디바이스가 사용할 수 있도록 허락한다는 정보를 포함한다. 디바이스가 컨텐츠에 대한 재생 권한을 갖고 있다는 것은 디바이스가 컨텐츠를 실행할 수

있는 유효한 권리 객체를 저장하고 있거나 권리 객체가 통합된 컨텐츠를 저장하고 있다 것을 의미할 수 있다.

<55> 이상에서 설명되지 않은 용어는 이하 필요한 부분에서 별도로 설명될 것이다.

<56> 도 1은 본 발명의 일 실시예에 따른 DRM 시스템(100)을 나타낸 도면이다. 도시된 DRM 시스템(100)은 메인 디바이스(110), 원격 디바이스(120), 서비스 제공 장치(130), 및 컨텐츠 공급 서버(140)를 포함한다.

<57> 메인 디바이스(110)는 유선 또는 무선으로 통신을 수행할 수 있으며, 플래쉬 메모리나 하드 디스크 등의 저장 매체를 포함하는 장치이다. 따라서 메인 디바이스(110)는 다른 장치에게 컨텐츠나 권리 객체를 송신하거나, 다른 장치로부터 컨텐츠나 권리 객체를 수신하고 이들을 저장할 수 있다. 물론 메인 디바이스(110)는 권리 객체를 소비하여 컨텐츠를 재생시킬 수도 있다. 또한, 메인 디바이스(110)는 원격 디바이스(120)에게 증명서를 발급해줄 수 있다. 메인 디바이스(110)의 일 실시예로써, PC(Personal Computer), 노트북, 셋탑박스, TV, PVR(Personal Video Recorder) 등을 들 수 있다.

<58> 원격 디바이스(120)는 유선 또는 무선으로 통신을 수행할 수 있으며, 컨텐츠를 재생시킬 수 있는 장치이다. 본 발명의 일 실시예에 따르면 원격 디바이스(120)는 컨텐츠와 권리 객체를 직접 저장하고 있지 않더라도 소정의 절차를 거치면 원격 디바이스(120)가 보유하고 있는 재생 권한에 대응하는 컨텐츠를 재생시킬 수 있다. 이를 위해서 원격 디바이스(120)는 메인 디바이스(110)로부터 발급 받은 증

명서를 사용할 수 있다. 원격 디바이스(120)의 일 실시예로서, 휴대폰, PDA(Personal Digital Assistants), PMP(Portable Multimedia Player), MP3 플레이어(MPEG audio layer-3 player) 등의 휴대용 단말기를 들 수 있다.

<59> 그러나 본 발명이 이에 한정되는 것은 아니며, 메인 디바이스(110)와 원격 디바이스(120)는 동종의 장치일 수도 있다.

<60> 컨텐츠 공급 서버(140)는 컨텐츠나 권리 객체를 제공한다. 만약, 컨텐츠와 권리 객체가 서로 독립된 개체로 존재한다면, 권리 객체는 일정한 대가를 지불한 디바이스에게 제공될 수 있을 것이며, 컨텐츠는 암호화된 상태로 대가 없이 제공될 수 있을 것이다. 이는, 암호화된 컨텐츠를 재생시키기 위해서는 권리 객체가 필요하기 때문이다. 물론, 권리 객체가 컨텐츠에 통합되어 있다면, 컨텐츠 공급 서버(140)는 일정한 대가를 지불한 디바이스에게 컨텐츠를 제공할 수 있을 것이다. 한편, 이상에서는 컨텐츠와 권리 객체가 동일 주체(컨텐츠 공급 서버(140))로부터 제공되는 것으로 설명하였으나, 컨텐츠와 권리 객체는 별개의 주체에 의해 제공될 수도 있다.

<61> 서비스 제공 장치(130)는 원격 디바이스로(140)의 요청에 따라서 메인 디바이스(110)가 재생 권한을 갖는 컨텐츠를 원격 디바이스(120)에 제공할 수 있다. 이를 위해 서비스 제공 장치(130)가 직접 컨텐츠를 저장하고 있을 수도 있으나, 서비스 제공 장치(130)는 컨텐츠 공급 서버(140)로부터 컨텐츠를 전달 받고 이를 다시 원격 디바이스(140)에게 제공하여 줄 수도 있다. 원격 디바이스(120)에게 제공되는 컨텐츠는 권리 객체 없이 재생할 수 있는 상태(예를 들어 컨텐츠 암호화키로

복호화된 상태의 컨텐츠)일 수 있다. 물론, 원격 디바이스(120)에게 전송되는 컨텐츠가 다른 장치에게 공개되는 것을 막기 위해서, 서비스 제공 장치(130)에 의한 소정의 보안 작업이 수행될 수 있다.

<62> 메인 디바이스(110)와 원격 디바이스(120) 간에는 블루투스, 무선랜, USB, IEEE 등 근거리 통신 프로토콜에 기반하여 필요한 데이터가 교환될 수 있으며, DRM 시스템(100)에서 나머지 장치들 간의 통신을 위해서는 xDSL, 전화선, 광 케이블 등에 기반한 원거리 통신 프로토콜이 사용될 수 있다. 물론, 본 발명이 이에 한정되는 것은 아니므로 DRM 시스템(100) 내의 장치들 간에 사용될 수 있는 통신 프로토콜은 실시예에 따라서 변형될 수 있다.

<63> 이러한 DRM 시스템(100)에 기반하여 사용자가 이용할 수 있는 컨텐츠 사용 시나리오의 일 예를 들면, 사용자는 가정에서 메인 디바이스(110)를 이용하여 컨텐츠 공급 서버(140)로부터 권리 객체 또는 컨텐츠를 구입한 후, 메인 디바이스(110)와 원격 디바이스(120)를 연결하여 메인 디바이스(110)가 생성한 증명서를 원격 디바이스(120)에 저장시킬 수 있다. 이 경우, 원격 디바이스(120)를 휴대한 사용자는 원격 디바이스를 통하여 서비스 제공 장치(130)에게 메인 디바이스(130)가 보유하고 있는 재생 권한에 대응하는 컨텐츠를 요청할 수 있다. 이 때, 서비스 제공 장치(130)는 일정 절차를 거친 후, 원격 디바이스(120)에게 컨텐츠를 제공할 수 있으며, 사용자는 원격 디바이스(120)를 통하여 컨텐츠를 사용할 수 있다. 즉, 사용자는 메인 디바이스(110)를 이용하여 구입한 컨텐츠나 권리 객체를 원격 디바이스(120)로 이동시키지 않더라도, 원격 디바이스(120)를 이용하여 필요한 컨텐츠를 재

생시킬 수 있게 된다.

<64> 한편, 도 1에서는 컨텐츠 공급 서버(140)와 서비스 제공 장치(130)가 독립적인 주체로 설명되고 있으나, 본 발명은 이에 한정되지 않으며 컨텐츠 공급 서버(140)와 서비스 제공 장치(130)는 동일 주체일 수도 있다.

<65> 이하에서는, DRM 시스템(100)의 장치들 간 동작 과정과 각 장치들의 구성에 대해서 보다 구체적으로 설명하도록 한다.

<66> 메인 디바이스(110), 원격 디바이스(120), 서비스 제공 장치(130), 및 컨텐츠 공급 서버(140)는 본격적인 통신을 수행하기 전에 상대 장치의 안전성을 확인하는 작업 및 인증 과정을 수행하는 것이 바람직하다. 상대 장치의 안전성을 확인하기 위해서 TCG(Trusted Computing Group) 표준의 어테스테이션 메커니즘(attestation mechanism)이 사용될 수 있다. 그러나 이는 예시적인 것이므로, 상대 장치의 안전성을 확인 하기 위해서 다른 방식이 사용될 수도 있다. 또, 상대 장치의 안전성을 확인하는 과정 없이 상대 장치와의 인증 과정이 수행될 수도 있다. 상대 장치와의 인증 과정의 일 예로, 도 2에 도시한 상호 인증 과정을 들 수 있다.

<67> 도 2는 본 발명의 일 실시예에 따른 상호 인증 과정을 나타낸 흐름도이다. 본 실시예에서 아래 첨자 '1'는 제1 장치(10) 소유이거나 제1 장치(10)가 생성한 데이터를 의미하고, 아래 첨자 '2'는 제2 장치(20) 소유이거나 제2 장치(20)가 생성한 데이터를 의미한다. 또한, 제1 장치(10)와 제2 장치(20)는 각각 메인 디바이스(110), 원격 디바이스(120), 서비스 제공 장치(130), 및 컨텐츠 공급 서버(140) 중 어느 하나일 수 있다.

<68> 먼저 제1 장치(10)와 제2 장치(20)가 연결되면, 제1 장치(10)는 제2 장치(20)에게 상호 인증을 요청한다(S210). 이 때 제1 장치(10)는 인증기관(Certification Authority)이 제1 장치(10)에 대하여 발행한 인증서$_1$를 함께 전송할 수 있다. 인증서$_1$는 제1 장치(10)의 ID_1와 공개키$_1$를 포함하고, 인증기관에 의하여 전자서명 되어 있다.

<69> 제1 장치(10)의 인증서$_1$를 수신한 제2 장치(210)는 인증서 폐기 목록(Certificate Revocation List; 이하, "CRL"이라 함)을 사용하여 인증서$_1$가 유효한 것인지를 확인한다(S212). 만약, 제1 장치(10)의 인증서$_1$가 CRL에 등록된 인증서라면, 제2 장치(20)는 제1 장치(10)와의 상호 인증을 거부할 수 있다. 그러나 제1 장치(10)의 인증서$_1$가 CRL에 등록되지 않은 인증서라면, 제2 장치(20)는 인증서$_1$를 통해서 제1 장치(10)의 공개키$_1$를 얻을 수 있다.

<70> 인증서$_1$ 확인을 통해서 제1 장치(10)가 정당한 장치인 것으로 판단되면 제2 장치(20)는 난수$_2$를 생성하고(S214), 생성된 난수$_2$를 제1 장치(10)의 공개키$_1$로 암호화한다(S216).

<71> 그 후, 제2 장치(20)은 상호인증 응답을 수행한다(S220). 상호인증 응답시 제2 장치(20)는 인증기관이 제2 장치(20)에 대하여 발행한 인증서$_2$ 및 암호화된 난수$_2$를 함께 전송시킬 수 있다. 인증서$_2$는 제2 장치(20)의 ID_2와 공개키$_2$를

포함하고, 인증기관에 의하여 전자서명 되어 있다.

<72> 제2 장치(20)로부터 인증서$_2$ 및 암호화된 난수$_2$를 수신한 제1 장치(10)는 인증서$_2$를 통해서 제2 장치(20)가 정당한 장치임을 확인하고 암호화된 난수$_2$를 제1 장치(10)의 개인키$_1$로 복호화 한다(S222). 이 때 제1 장치(10)는 제2 장치(20)의 인증서$_2$를 통해서 제2 장치(20)의 공개키$_2$를 획득할 수 있다. 또한 인증서$_2$에 대한 확인 작업은 제2 장치(20)와 마찬가지로 CRL을 통해서 수행될 수 있다.

<73> 인증서$_2$ 확인을 통해서 제2 장치(20)가 정당한 장치인 것으로 판단되면 제1 장치(10)는 난수$_1$를 생성하고(S224), 생성된 난수$_1$를 제2 장치(20)의 공개키$_2$로 암호화한다(S226).

<74> 그 후, 제1 장치(10)는 제2 장치(20)에게 상호인증 종료를 요청한다(S230). 상호인증 종료 요청 시 제1 장치(10)는 암호화된 난수$_1$를 함께 전송한다.

<75> 제1 장치(10)로부터 암호화된 난수$_1$를 수신한 제2 장치(20)는 자신의 개인키$_2$로 암호화된 난수$_1$를 복호화 한다(S232).

<76> 이에 따라서 제1 장치(10)와 제2 장치(20)는 상호 두개의 난수(난수$_1$ 및 난수$_2$)를 공유하게 된다.

<77> 상호인증 결과 두개의 난수(난수$_1$ 및 난수$_2$)를 공유한 제1 장치(10)와 제2 장

치(20)는 두개의 난수(난수$_1$ 및 난수$_2$)를 사용하여 세션키를 생성한다(S240, S242). 이 때 제1 장치(10)와 제2 장치(20)가 세션키를 생성하기 위해서 사용하는 키생성 알고리즘은 상호 동일하다. 따라서 제1 장치(10)와 제2 장치(20)는 상호 동일한 세션키를 공유할 수 있게 된다.

<78> 제1 장치(10)와 제2 장치(20)는 상호인증 이후 상대방에게 전송할 데이터를 세션키로 암호화하고, 상대방으로부터 수신된 암호화된 데이터를 세션키로 복호화 할 수 있다. 이에 따라서 제1 장치(10)와 제2 장치(20) 간의 데이터 전송에 보안이 유지될 수 있다. 이하의 각 실시예에서 특별한 언급이 없더라도 제1 장치(10)와 제2 장치(20)는 상대방에게 송신할 데이터를 상호인증 결과 생성된 세션키로 암호화 하고, 상대방으로부터 수신된 암호화된 데이터를 세션키로 복호화 하는 것으로 이해할 수 있다.

<79> 한편, 도 2의 흐름도에서는 제1 장치(10)와 제2 장치(20)가 세션키를 생성하기 위해서 난수를 교환하는 과정과 세션키를 생성하는 과정까지 설명하였지만, 세션키 생성이 필요 없다면 난수 생성 및 교환 과정과 세션키 생성 과정은 생략 될 수 있다. 즉, 상대 장치의 정당성만을 확인하고자 한다면, 상대 장치로부터 전송되는 인증서를 검증하는 것으로 상호 인증 과정이 마쳐질 수 있다.

<80> 도 3은 본 발명의 일 실시예에 따른 원격 디바이스(120)가 메인 디바이스(100)로부터 증명서를 발급 받는 과정을 나타낸 흐름도이다.

<81> 먼저, 원격 디바이스(120)는 메인 디바이스(110)에게 증명서 발급을 요청한

다(S310). 증명서 발급이 요청될 때 메인 디바이스(110)는 원격 디바이스(120)의 안정성 유무를 검증할 수 있는데, 이를 위하여 앞서 언급한 바와 같이 TCG 표준의 인증 메커니즘(attestation mechanism)이나, 도 2의 상호 인증(authentication) 과정이 사용될 수 있다. 따라서, 원격 디바이스(120)는 증명서 발급 요청 시 자신의 식별자(예를 들어 MAC 주소)나 인증서(certificate) 등을 메인 디바이스에게 전송할 수 있다. 물론 안정성 확인 작업은 증명서 발급 요청 이전에 선행될 수도 있다.

<82> 만약 원격 디바이스(120)가 안전한 디바이스로 인정된다면, 메인 디바이스(110)는 원격 디바이스(120)에게 발급할 증명서를 생성한다(S320). 증명서는 발급하는 주체와 발급 받는 대상에 대한 정보를 포함하는 것이 바람직하다. 본 발명의 일 실시예로서 증명서는 원격 디바이스(120)의 식별자와 메인 디바이스(110)의 식별자를 포함할 수 있다. 다른 예로서, 증명서는 원격 디바이스(120)의 공개키와 메인 디바이스(110)의 공개키를 포함할 수도 있다. 생성된 증명서는 메인 디바이스(110)의 개인키로 암호화되는 것이 바람직하다. 이는 증명서가 메인 디바이스(110)에 의해 생성된 것임을 제3의 장치가 확인할 수 있도록 하기 위함이다.

<83> 증명서를 발급하여 준다는 것은 메인 디바이스(110)는 자신이 보유하고 있는 재생 권한의 전부 또는 일부를 원격 디바이스(120)게 나누어 준다는 것을 의미한다. 만약, 메인 디바이스(110)가 자신이 갖고 있는 재생 권한의 일부만 원격 디바이스(120)에게 할당하여 주고자 한다면, 메인 디바이스(110)는 증명서에 제한된 권한에 대한 정보를 포함시킬 수 있다. 이하, 증명서에 포함되는 제한된 권

한에 대한 정보를 앞선 용어의 설명에서 권리 객체의 구성으로 설명한 제한 정보와 구분하기 위하여, 사용 한도 정보라 한다.

<84> 예를 들어, 메인 디바이스(110)가 컨텐츠를 10회 재생시킬 수 있는 권한을 갖고 있고, 원격 디바이스(120)에게 컨텐츠를 2회 재생시킬 수 있는 권한을 허락한다면, 메인 디바이스(110)는 컨텐츠를 2회 재생할 수 있다는 사용 한도 정보를 포함하는 증명서를 생성할 수 있다.

<85> 증명서에 포함되는 사용 한도 정보의 범위는 원격 디바이스(120)의 요청에 따른 것이거나, 원격 디바이스(120)의 요청 없이 메인 디바이스(110)가 할당한 것일 수 있다.

<86> 증명서가 생성되면 메인 디바이스(110)는 원격 디바이스(120)에게 증명서를 전송한다(S330).

<87> 그 후, 메인 디바이스(110)는 증명서를 이용하여 재생할 수 있는 컨텐츠의 목록(이하 컨텐츠 목록이라 한다)을 원격 디바이스(120)에게 전송한다(S340). 컨텐츠 목록은 컨텐츠를 식별할 수 있는 컨텐츠 식별자, 컨텐츠 유형(예를 들어 동영상, 음악, 게임, 사진 등), 등 컨텐츠에 대한 세부 정보를 포함할 수 있다. 컨텐츠 목록은 메인 디바이스가 재생 권한을 갖는 모든 컨텐츠에 대한 정보를 포함할 수도 있지만, 그 중 일부 컨텐츠에 대한 정보를 포함할 수도 있다. 또한, 컨텐츠 목록은 사전에 작성된 것일 수도 있지만, 증명서 발급 시 작성된 것일 수도 있다.

<88> 메인 디바이스(110)로부터 증명서를 발급 받은 원격 디바이스(120)는 컨텐츠

나 권리 객체를 저장하고 있지 않더라도 소정의 절차를 거쳐서 컨텐츠를 재생시킬 수 있는데, 이에 대해서 도 4를 참조하여 설명하도록 한다.

<89> 도 4는 본 발명의 일 실시예에 따른 원격 디바이스(120)의 컨텐츠 재생 과정을 나타낸 흐름도이다.

<90> 메인 디바이스(110)로부터 증명서를 발급 받은 원격 디바이스(120)는 서비스 제공 장치(130)에게 컨텐츠 사용을 요청한다(S410). 이 때, 원격 디바이스(120)는 메인 디바이스(110)로부터 발급 받은 증명서와 사용하고자 하는 컨텐츠에 대한 정보(예를 들어 컨텐츠 식별자)를 전송할 수 있다. 사용하고자 하는 컨텐츠에 대한 정보는 메인 디바이스(110)로부터 전달 받은 컨텐츠 목록 중에서 선택 가능하다.

<91> 원격 디바이스(120)로부터 컨텐츠 사용 요청이 수신되면, 서비스 제공 장치(130)는 컨텐츠 사용 요청과 함께 전송된 증명서를 검증한다(S415). 증명서는 메인 디바이스(110)의 개인키로 암호화되어 있기 때문에, 메인 디바이스(110)의 공개키를 사용하여 암호화된 증명서를 복호화할 수 있다면 증명서가 메인 디바이스(110)에 의해 발급된 것임을 확인할 수 있다. 메인 디바이스(110)의 공개키는 인증 기관으로부터 제공 받거나, 메인 디바이스(110)로부터 직접 제공 받을 수 있다. 또는 원격 디바이스(120)로부터 컨텐츠 사용 요청과 함께 메인 디바이스(110)의 인증서를 전달 받을 수도 있는데, 이 경우 서비스 제공 장치(130)는 메인 디바이스(110)의 인증서를 통하여 메인 디바이스(110)의 공개키를 획득할 수 있다. 이 밖에도 다양한 루트를 통하여 메인 디바이스(110)의 공개키를 획득하는 것이 가능하다. 또한, 메인 디바이스(110)의 공개키 이외에 증명서를 검증하기 위해 다른 정

보가 필요하다면, 이 또한 메인 디바이스(110), 원격 디바이스(120), 또는 제3의 장치 등으로부터 획득할 수 있다.

<92> 도시되지는 않았으나, 원격 디바이스(120)로부터 전송된 증명서가 적법하지 않다면, 서비스 제공 장치(130)는 원격 디바이스(120)에게 컨텐츠를 제공할 수 없음을 알릴 수 있다.

<93> 그러나, 증명서가 적법한 것으로 검증된다면 서비스 제공 장치(130)는 메인 디바이스(110)의 구매 이력을 점검한다(S420). 구매 이력은 메인 디바이스(110)가 컨텐츠 공급 서버(140)로부터 구매한 권리 객체나 컨텐츠에 대한 정보를 포함할 수 있다. 구매 이력을 점검함으로써 서비스 제공 장치(130)는 원격 디바이스(120)가 요청한 컨텐츠에 대한 재생 권한이 메인 디바이스(110)에게 있는지를 확인할 수 있다.

<94> 메인 디바이스(110)의 구매 이력은 컨텐츠 공급 서버(140)로부터 획득할 수 있다. 물론, 메인 디바이스(110)가 컨텐츠 공급 서버(140)로부터 권리 객체나 권리 객체가 포함된 컨텐츠를 구매할 때마다 컨텐츠 공급 서버(140)가 구매 내역을 서비스 제공 장치(130)로 전달함으로써, 서비스 제공 장치(130)가 메인 디바이스(110)의 구매 이력을 생성 및 관리하는 실시예도 가능하다.

<95> 구매 이력 점검 결과, 원격 디바이스(120)가 요청한 컨텐츠에 대한 메인 디바이스(110)의 재생 권한이 확인되면, 서비스 제공 장치(130)는 메인 디바이스(110)에게 권리 객체의 상태 정보를 갱신할 것을 요청한다(S425). 이 때, 서비스 제공 장치(130)는 원격 디바이스가 요청한 컨텐츠에 대한 정보(예를 들어 컨텐츠

식별자)를 메인 디바이스(110)에게 제공할 수 있다.

<96> 과정 S425에서 상태 정보의 갱신 정도는 원격 디바이스(120)로부터 전송된 증명서에 포함된 사용 한도 정보에 대응될 수 있다. 예를 들어, 사용 한도 정보가 컨텐츠의 2회 재생을 허여한다는 정보라면, 서비스 제공 장치(130)는 해당 컨텐츠에 대응하는 권리 객체의 상태 정보를 2회만큼 카운트할 것을 메인 디바이스(110)에게 요청할 수 있다.

<97> 본 발명의 일 실시예에 따르면, 과정 S425에서 요청되는 상태 정보의 갱신 정도는 원격 디바이스(120)에 의해 결정될 수도 있다. 예를 들어, 원격 디바이스(120)는 과정 S410에서의 컨텐츠 사용 요청 시 컨텐츠 사용량에 대한 정보도 전송할 수 있다. 이 때, 서비스 제공 장치(130)는 컨텐츠 사용량에 대한 정보가 증명서에 포함된 사용 한도 정보 이내에 속하는지 판단하고, 그러하다면 과정 S425에서 원격 디바이스(120)가 요구한 컨텐츠 사용량만큼 상태 정보를 갱신 하도록 메인 디바이스(110)에게 요청할 수 있다. 예를 들어 원격 디바이스(120)가 컨텐츠의 1회 사용을 요청하였다면, 서비스 제공 장치(130)는 메인 디바이스(110)에게 해당 컨텐츠의 권리 객체에서 횟수 제한에 대한 상태 정보를 1회 카운트하도록 요청할 수 있다.

<98> 다시 도 4를 참조하면, 메인 디바이스(110)는 서비스 제공 장치(130)의 요청에 따라서 권리 객체의 상태 정보를 갱신한다(S430). 상태 정보가 갱신되어야 할 권리 객체는, 상태 정보 갱신 요청과 함께 수신된 컨텐츠에 대한 정보를 통해서 검색될 수 있다. 본 발명의 일 실시예에 따르면, 메인 디바이스(110)는 상태 정보를

갱신하기 전에 서비스 제공 장치(130)에게 증명서를 요청할 수도 있다. 이 경우, 서비스 제공 장치(130)는 원격 디바이스(120)로부터 전송 받은 증명서를 메인 디바이스(110)에게 전송하고, 메인 디바이스(110)는 이를 자신의 공개키로 복원함으로써, 서비스 제공 장치(130)의 상태 정보 갱신 요청이 정당함을 확인할 수 있다.

<99> 상태 정보를 갱신한 한 후, 메인 디바이스(110)는 상태 정보의 갱신을 확인시키기 위한 응답 패킷을 생성하고(S435), 이를 서비스 제공 장치(130)에게 전송한다(S440). 여기서 응답 패킷은 갱신 전의 상태 정보와 갱신된 상태 정보를 포함할 수 있으며, 메인 디바이스(110)의 개인키로 암호화되어 있을 수 있다. 만약, 서비스 제공 장치(130)에게 받은 상태 정보 갱신 요청이 메인 디바이스(110)가 가지고 있는 상태 정보의 허용 범위를 넘을 경우에는 응답 패킷에 '컨텐츠 사용 불가'와 같은 거절 내용이 포함될 수 있다. 예를 들어, 원격 디바이스(120)가 서비스 제공 장치(130)에게 컨텐츠를 5회 재생을 요청하고, 요청을 받은 서비스 제공 장치(130)는 메인 디바이스(110)에게 상태 정보 갱신(상태 정보에서 5회 재생을 감소)을 요청할 수 있다. 이 경우, 상태 정보 갱신 요청을 받은 메인 디바이스(110)가 보유한 상기 컨텐츠에 대한 재생 권한이 4회라면, 메인 디바이스(110)가 허락할 수 있는 권한의 범위보다 요청 받은 상태 정보 갱신 범위가 더 크기 때문에 메인 디바이스(110)는 '권한 범위보다 큰 요청임' 등과 같은 내용을 포함하는 응답 패킷을 생성하여, 서비스 제공 장치(130)에게 전송할 수 있다.

<100> 서비스 제공 장치(130)는 메인 디바이스(110)로부터 수신된 응답 패킷을 통해서 상태 정보의 갱신 여부를 확인한다(S445). 예를 들어, 메인 디바이스(110)의

공개키로 응답 패킷이 복호화되고, 복호화된 응답 패킷의 내용이 상태 정보가 갱신되었음을 지시하고 있는 경우, 서비스 제공 장치(130)는 상태 정보가 성공적으로 갱신 되었다고 판단할 수 있다.

<101> 상태 정보가 갱신되었다면 서비스 제공 장치(130)는 원격 디바이스(120)에게 컨텐츠를 제공할 수 있다(S450). 컨텐츠의 제공은 스트리밍 형식 또는 다운로드 형식으로 수행될 수 있다. 다운로드 형식의 경우, 컨텐츠와 함께 컨텐츠의 재생 한도를 제한하는 임계값도 함께 전송될 수 있다. 이 경우, 원격 디바이스(120)가 컨텐츠를 재생시킬 때마다 재생 한도를 제한하는 임계값이 갱신된다. 예를 들어 재생 한도를 제한하는 임계값이 2회로 설정되어 있다면, 원격 디바이스(120)가 컨텐츠를 재생할 경우 임계값이 카운팅되므로 원격 디바이스(120)는 총 2회만큼 컨텐츠를 재생시킬 수 있게 된다. 재생 한도를 제한하는 임계값은 과정 S430에서의 상태 정보 갱신 정도에 대응하는 값을 갖는다.

<102> 한편, 과정 S450에서 전송되는 컨텐츠는 원격 디바이스(120)와 서비스 제공 장치(130)에 의해 공유된 정보를 사용하여 암호화된 상태일 수 있다. 예를 들어, 서비스 제공 장치(130)는 원격 디바이스(120) 고유의 공개키나 원격 디바이스(120)의 식별자를 이용하여 컨텐츠를 암호화할 수 있다. 만약, 도 2에 도시된 바와 같은 상호인증 과정이 선행되었다면, 서비스 제공 장치(130)는 상호 인증 결과 생성된 세션키를 사용하여 컨텐츠를 암호화할 수도 있다. 컨텐츠의 암호화를 통해서 컨텐츠가 원격 디바이스(120)이외의 디바이스에 의해 사용되는 것을 방지할 수 있다.

<103> 서비스 제공 장치(130)로부터 컨텐츠를 제공 받은 원격 디바이스(120)는 컨텐츠를 재생할 수 있다(S455).

<104> 도 5는 본 발명의 일 실시예에 따른 메인 디바이스(110)를 나타낸 블록도이다. 메인 디바이스(110)는 통신부(510), 저장부(520), 컨텐츠 목록 생성부(530), 증명서 생성부(540), 응답 패킷 생성부(550), 및 제어부(560)를 포함한다.

<105> 통신부(510)는 유선 또는 무선 매체를 통하여 외부 장치와 데이터를 송수신한다. 보다 구체적으로 통신부(510)는 제1 인터페이스부(512)와 제2 인터페이스부(514)를 포함할 수 있다. 제1 인터페이스부(512)는 적외선 통신, 블루투스, 무선랜, USB, IEEE1394 등의 통신 프로토콜을 이용하여 근거리 통신을 수행할 수 있으며, 제2 인터페이스부(514)는 xDSL, 광케이블, 전화선 등에 기반한 통신 프로토콜을 이용하여 원거리 통신을 수행할 수 있다. 바람직하게는 제1 인터페이스부(512)는 원격 디바이스(120)와의 통신을 위해 사용될 수 있으며, 제2 인터페이스부(514)는 컨텐츠 공급 서버(140)나 서비스 제공 장치(130)와의 통신을 위해 사용될 수 있다.

<106> 저장부(520)는 하드 디스크나 플래쉬 메모리 등의 저장 매체를 포함하며, 컨텐츠나 권리 객체를 저장할 수 있다. 바람직하게는 권리 객체나 컨텐츠와 같이 강력한 보안이 요구되는 데이터는 일반 데이터가 저장되는 저장 영역으로부터 논리적 또는 물리적으로 구분된 보안 저장 영역에 저장된다. 보안 저장 영역으로의 접근은 제어부(560)에 의해서 가능하며, 외부 장치나 제 3의 모듈에 의한 접근은 차단되는 것이 바람직하다.

<107> 컨텐츠 목록 생성부(530)는 앞서 설명한 컨텐츠 목록을 작성한다. 컨텐츠 목록은 원격 디바이스(120)로부터 증명서 요청이 수신된 경우에 작성될 수도 있지만, 저장부(520)에 새로운 권리 객체를 저장하거나 저장부(530)에 저장되었던 권리 객체가 삭제되는 등 재생 권한의 변동에 따라서 컨텐츠 목록을 상시 업데이트하여 둘 수도 있다.

<108> 증명서 생성부(540)는 원격 디바이스(120)에게 제공할 증명서를 생성한다.

<109> 응답 패킷 생성부(550)는 서비스 제공 장치(130)의 요청에 따라서 상태 정보가 갱신될 경우 이를 확인할 수 있는 정보를 포함하는 응답 패킷을 생성한다. 일예로서, 응답 패킷은 갱신 전과 갱신 후의 상태 정보를 포함할 수 있다.

<110> 제어부(560)는 메인 디바이스(110)를 구성하는 각 구성요소들의 동작을 제어한다. 또한, 제어부(560)는 메인 디바이스(110)의 보안을 유지하며, DRM 매니저로서 기능할 수 있다. 예를 들어 제어부(560)는 권리 객체의 상태 정보를 갱신하고, 각종 암호화 및 복호화 작업을 수행할 수 있으며, 다른 장치와의 통신 시 상대 장치의 안정성 검사 과정을 제어할 수 있다.

<111> 도 6은 본 발명의 일 실시예에 따른 원격 디바이스(120)를 나타낸 블록도이다. 원격 디바이스(120)는 통신부(610), 저장부(620), 증명서 발급 요청부(630), 재생부(640), 및 제어부(650)를 포함한다.

<112> 통신부(610)는 유선 또는 무선 매체를 통하여 외부 장치와 데이터를 송수신한다. 통신부(610)의 구성은 도 5를 참조하여 설명한 메인 디바이스(110)의 통신

부(510)의 구성과 유사하게 이해될 수 있다. 제1 인터페이스부(612)는 메인 디바이스(110)와의 통신을 위해 사용되고, 제2 인터페이스부(614)는 서비스 제공 장치(130)와의 통신을 위해 사용되는 것이 바람직하다.

<113> 저장부(620)는 하드 디스크나 플래쉬 메모리 등의 저장 매체를 포함하며, 메인 디바이스(110)로부터 전달 받은 증명서나 서비스 제공 장치(130)로부터 전달 받은 컨텐츠 등을 저장할 수 있다. 바람직하게는 저장부(620)는 외부 장치나 제 3의 모듈에 의한 접근으로부터 논리적 또는 물리적으로 보호될 수 있으며, 제어부(650)의 제어에 따라서 데이터가 저장, 삭제, 변경, 또는 인출될 수 있다.

<114> 요청부(630)는 증명서 발급 요청과 컨텐츠 요청 작업을 관리한다. 이를 위해, 요청부(630)는 증명서 발급 요청 패킷과 컨텐츠 요청 패킷을 생성하고, 그에 대한 응답으로서 수신되는 패킷이나 정보를 처리할 수 있다.

<115> 재생부(640)는 서비스 제공 장치(130)로부터 제공된 컨텐츠를 재생한다. 예를 들어 재생부(640)는 MPEG 디코더를 포함하여 동영상을 재생시킬 수 있다.

<116> 제어부(650)는 원격 디바이스(120)를 구성하는 각 구성요소들의 동작을 제어한다. 또한, 제어부(650)는 원격 디바이스(110)의 보안을 유지하며, DRM 매니저로서 기능할 수 있다. 예를 들어, 제어부(560) 각종 암호화 및 복호화 작업을 수행하고, 다른 장치와의 통신 시 상대 장치의 안정성 검사 과정을 제어할 수 있다. 또한, 서비스 제공 장치(130)로부터 제공되는 컨텐츠에 재생 한도를 제한하는 임계값이 설정되어 있다면, 제어부(650)는 임계값으로 정의되는 한도 내에서 재생부(640)가 컨텐츠를 재생할 수 있도록 제어할 수 있다.

<117> 도 7은 본 발명의 일 실시예에 따른 서비스 제공 장치(130)를 나타낸 블록도이다. 서비스 제공 장치(130)는 통신부(710), 구매 이력 검사부(720), 증명서 검증부(730), 상태 정보 갱신 검증부(740), 컨텐츠 제공부(750), 및 제어부(760)를 포함한다.

<118> 통신부(710)는 유선 또는 무선 매체를 통하여 외부 장치와 데이터를 송수신한다. 예를 들어 통신부(710)는 xDSL, 광케이블, 전화선 등에 기반한 통신 프로토콜을 이용하여 메인 장치(110), 원격 장치(120), 및 컨텐츠 공급 서버(140)와 통신을 수행할 수 있다.

<119> 구매 이력 검사부(720)는 메인 디바이스(110)의 구매 이력을 검사한다. 이를 위해 구매 이력 검사부(720)는 컨텐츠 공급 서버(140)에게 메인 디바이스(110)의 구매 이력을 요청하고, 그에 대한 응답으로서 컨텐츠 공급 서버(140)로부터 메인 디바이스(110)의 구매 이력을 제공 받을 수 있다. 본 발명의 일 실시예에 따르면, 구매 이력 검사부(720)는 주기적 또는 비주기적으로 컨텐츠 공급 서버(140)로부터 메인 디바이스(110)의 컨텐츠나 권리 객체 구매 내역을 제공 받음으로써, 메인 디바이스(110)의 구매 이력을 직접 관리할 수도 있다.

<120> 증명서 검증부(730)는 원격 디바이스(120)로부터 전송된 증명서의 정당성 여부를 검증한다. 예를 들어, 메인 디바이스(110)의 공개키를 사용하여 증명서가 복호화될 경우, 증명서 검증부(730)는 증명서가 정당한 것으로 판단할 수 있다.

<121> 상태 정보 갱신 검증부(740)는 원격 디바이스(120)로부터 컨텐츠 전송 요청이 수신된 경우, 메인 디바이스(110)에게 해당 컨텐츠에 대응하는 권리 객체의 상

태 정보를 갱신할 것을 요청하고, 그에 대한 응답으로서 메인 디바이스(110)로부터 전송된 응답 패킷을 통해서 상태 정보가 정상적으로 갱신 되었는지의 여부를 검사한다.

<122> 컨텐츠 제공부(750)는 원격 디바이스(120)가 요청한 컨텐츠를 원격 디바이스(120)에게 제공한다. 컨텐츠의 제공은 스트리밍이나 다운로드 방식일 수 있다. 물론, 원격 디바이스(120)에게 컨텐츠를 제공하기까지는 도 4를 참조하여 설명한 바와 같은 과정들 수행될 것이며, 각 과정들이 성공적으로 수행될 경우 컨텐츠가 제공될 수 있다. 필요한 컨텐츠를 적절히 제공하기 위해서, 컨텐츠 제공부(750)는 컨텐츠 공급 서버(140)와 연동되어 컨텐츠 공급 서버(140)로부터 제공되는 컨텐츠를 원격 디바이스(120)에게 다시 제공할 수 있다. 물론, 컨텐츠 제공부(750)는 컨텐츠를 저장하는 별도의 데이터 베이스를 관리하고, 데이터 베이스에서 필요한 컨텐츠를 검색하여 원격 디바이스(120)에게 제공할 수도 있다.

<123> 제어부(760)는 서비스 제공 장치(130)를 구성하는 각 구성요소들의 동작을 제어한다. 또한, 제어부(760)는 서비스 제공 장치(130)의 보안을 유지하며, DRM 매니저로서 기능할 수 있다. 예를 들어, 제어부(760) 각종 암호화 및 복호화 작업을 수행하고, 다른 장치와의 통신 시 상대 장치의 안정성 검사 과정을 제어할 수 있다. 또한, 제어부(760)는 원격 디바이스(120)에게 제공할 컨텐츠에 재생 한도를 제한하는 임계값을 포함시킬 수 있다.

<124> 이상의 설명에서 메인 디바이스(110), 원격 디바이스(120), 및 서비스 제공 장치(130)를 구성하는 각 구성요소들은 모듈로 구현될 수 있다. 상기 '모듈'은 소

프트웨어 또는 Field Programmable Gate Array(FPGA) 또는 주문형 반도체 (Application Specific Integrated Circuit, ASIC)과 같은 하드웨어 구성요소를 의미하며, 모듈은 어떤 역할들을 수행한다. 그렇지만 모듈은 소프트웨어 또는 하드웨어에 한정되는 의미는 아니다. 모듈은 어드레싱할 수 있는 저장 매체에 있도록 구성될 수도 있고 하나 또는 그 이상의 프로세서들을 실행시키도록 구성될 수도 있다. 따라서, 일 예로서 모듈은 소프트웨어 구성요소들, 객체지향 소프트웨어 구성요소들, 클래스 구성요소들 및 태스크 구성요소들과 같은 구성요소들과, 프로세스들, 함수들, 속성들, 프로시저들, 서브루틴들, 프로그램 코드의 세그먼트들, 드라이버들, 펌웨어, 마이크로코드, 회로, 데이터, 데이터베이스, 데이터 구조들, 테이블들, 어레이들, 및 변수들을 포함한다. 구성요소들과 모듈들에서 제공되는 기능은 더 작은 수의 구성요소들 및 모듈들로 결합되거나 추가적인 구성요소들과 모듈들로 더 분리될 수 있다.

<125> 도 5 내지 도 7을 참조하여 설명한 메인 디바이스(110), 원격 디바이스(120), 및 서비스 제공 장치(130)를 구성하는 구성 요소들 간의 유기적인 동작 과정은 도 1 내지 도 4를 참조하여 설명한 내용을 통해서 보다 구체적으로 이해될 수 있을 것이다.

<126> 이상과 첨부된 도면을 참조하여 본 발명의 실시예를 설명하였지만, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자는 본 발명이 그 기술적 사상이나 필수적인 특징을 변경하지 않고서 다른 구체적인 형태로 실시될 수 있다는 것을 이해할 수 있을 것이다. 그러므로 이상에서 기술한 실시예들은 모든 면에서 예시적

인 것이며 한정적이 아닌 것으로 이해해야만 한다.

【발명의 효과】

<127> 상기한 바와 같은 본 발명의 디지털 저작권 관리 방법 및 장치에 따르면 디지털 저작권을 보호하면서도 디바이스에 국한되지 않고 보다 유연하게 컨텐츠를 사용할 수 있는 효과가 있다.

【특허청구범위】

【청구항 1】

원격 디바이스의 디지털 저작권 관리 방법으로서,

컨텐츠에 대한 재생 권한을 갖는 메인 디바이스로부터 상기 컨텐츠의 사용을 허가한다는 정보를 포함하는 증명서를 발급 받는 단계;

상기 증명서를 서비스 제공 장치에게 전송하는 단계; 및

상기 서비스 제공 장치로부터 상기 컨텐츠를 제공 받는 단계를 포함하는, 디지털 저작권 관리 방법.

【청구항 2】

제 1항에 있어서,

상기 증명서는 상기 메인 디바이스에 대한 정보와 상기 원격 디바이스에 대한 정보 중 적어도 하나를 포함하는, 디지털 저작권 관리 방법.

【청구항 3】

제 2항에 있어서,

상기 메인 디바이스에 대한 정보는 상기 메인 디바이스의 식별자와 공개키 중 적어도 하나를 포함하고, 상기 원격 디바이스에 대한 정보는 상기 원격 디바이스의 식별자와 공개키 중 적어도 하나를 포함하는, 디지털 저작권 관리 방법.

【청구항 4】

제 1항에 있어서,

상기 증명서는 상기 컨텐츠에 대한 사용 한도 정보를 포함하는, 디지털 저작권 관리 방법.

【청구항 5】

제 1항에 있어서,

상기 증명서는 상기 메인 디바이스의 개인키로 암호화되어 있는, 디지털 저작권 관리 방법.

【청구항 6】

제 1항에 있어서,

상기 메인 디바이스로부터 상기 증명서를 이용하여 재생할 수 있는 컨텐츠의 목록을 수신하는 단계를 더 포함하고,

상기 서비스 제공 장치로부터 제공 받는 컨텐츠는 상기 목록에서 상기 원격 디바이스가 선택한 컨텐츠인, 디지털 저작권 관리 방법.

【청구항 7】

제 1항에 있어서,

상기 서비스 제공 장치로부터 제공 받는 컨텐츠는 상기 컨텐츠의 재생 한도를 제한하는 임계값을 포함하는, 디지털 저작권 관리 방법.

【청구항 8】

제 1항에 있어서,

상기 서비스 제공 장치로부터 제공 받는 컨텐츠는 상기 원격 디바이스와 상

기 서비스 제공 장치에 의해 공유된 정보를 통해 암호화된, 디지털 저작권 관리 방법.

【청구항 9】

제 8항에 있어서,

상기 공유된 정보는 상기 원격 디바이스의 식별자와 상기 원격 디바이스의 공개키 중 적어도 하나를 포함하는, 디지털 저작권 관리 방법.

【청구항 10】

컨텐츠에 대한 재생 권한을 갖는 메인 디바이스의 디지털 저작권 관리 방법으로서,

상기 컨텐츠의 사용을 허가한다는 정보를 포함하는 증명서를 원격 디바이스에게 발급하는 단계;

상기 원격 디바이스에게 상기 컨텐츠를 제공하려는 서비스 제공 장치로부터 상기 컨텐츠를 재생시킬 수 있는 권리 객체의 상태 정보를 갱신할 것을 요청 받는 단계; 및

상기 상태 정보를 갱신하는 단계를 포함하는, 디지털 저작권 관리 방법.

【청구항 11】

제 10항에 있어서,

상기 증명서를 이용하여 재생할 수 있는 컨텐츠의 목록을 상기 원격 디바이스에게 전송하는 단계를 더 포함하고,

상기 상태 정보의 갱신 대상이 되는 권리 객체는 상기 컨텐츠는 상기 목록에 존재하는 컨텐츠인, 디지털 저작권 관리 방법.

【청구항 12】

제 10항에 있어서,

상기 상태 정보가 갱신되었음을 나타내는 정보를 포함하는 응답 패킷을 상기 서비스 제공 장치에게 전송하는 단계를 더 포함하는, 디지털 저작권 관리 방법.

【청구항 13】

제 12항에 있어서,

상기 응답 패킷은 상기 메인 디바이스의 개인키로 암호화된, 디지털 저작권 관리 방법.

【청구항 14】

제 10항에 있어서,

상기 서비스 제공 장치가 상기 원격 디바이스로부터 획득한 상기 증명서를 상기 서비스 제공 장치로부터 수신하는 단계를 더 포함하고,

상기 상태 정보를 갱신하는 단계는 상기 증명서가 상기 메인 디바이스에 의해 발급된 것일 경우 수행되는, 디지털 저작권 관리 방법.

【청구항 15】

제 10항에 있어서,

상기 증명서는 상기 메인 디바이스의 개인키로 암호화된, 디지털 저작권 관

리 방법.

【청구항 16】

제 10항에 있어서,

상기 증명서는 상기 메인 디바이스에 대한 정보와 상기 원격 디바이스에 대한 정보 중 적어도 하나를 포함하는, 디지털 저작권 관리 방법.

【청구항 17】

제 10항에 있어서,

상기 증명서는 상기 컨텐츠에 대한 사용 한도 정보를 포함하는, 디지털 저작권 관리 방법.

【청구항 18】

서비스 제공 장치의 디지털 저작권 관리 방법으로서,

원격 디바이스로부터 증명서 및 컨텐츠 전송 요청을 수신하는 단계;

상기 증명서가 메인 디바이스에 의해 발급되었는지의 여부를 검증하는 단계; 및

상기 증명서가 상기 메인 디바이스에 의해 발급된 것일 경우, 상기 컨텐츠를 상기 원격 디바이스에게 제공하는 단계를 포함하는, 디지털 저작권 관리 방법.

【청구항 19】

제 18항에 있어서,

상기 메인 디바이스의 구매 이력을 검사하는 단계를 더 포함하고,

상기 제공하는 단계는 상기 메인 디바이스가 상기 컨텐츠 또는 상기 컨텐츠에 대응하는 권리 객체를 구매한 이력이 확인된 경우에 수행되는, 디지털 저작권 관리 방법.

【청구항 20】

제 18항에 있어서,

상기 메인 디바이스에게 상기 컨텐츠를 재생시킬 수 있는 권리 객체의 상태 정보를 갱신할 것을 요청하는 단계; 및

상기 상태 정보가 갱신되었다는 정보를 포함하는 응답 패킷을 상기 메인 디바이스로부터 수신하는 단계를 더 포함하고,

상기 제공하는 단계는, 상기 응답 패킷을 통하여 상기 상태 정보가 갱신된 것으로 판단된 경우에 수행되는, 디지털 저작권 관리 방법.

【청구항 21】

제 18항에 있어서,

상기 원격 디바이스에게 전송되는 컨텐츠는 상기 서비스 제공 장치와 상기 원격 디바이스 간에 공유된 정보로 암호화된, 디지털 저작권 관리 방법.

【청구항 22】

제 21항에 있어서,

상기 공유된 정보는 상기 원격 디바이스의 식별자와 상기 원격 디바이스의 공개키 중 적어도 하나를 포함하는, 디지털 저작권 관리 방법.

【청구항 23】

제 18항에 있어서,

상기 전송하는 단계는 상기 컨텐츠의 재생 한도를 제한하는 임계값을 포함하는, 디지털 저작권 관리 방법.

【청구항 24】

디지털 저작권 관리를 위한 원격 디바이스로서,

컨텐츠에 대한 재생 권한을 갖는 메인 디바이스로부터 상기 컨텐츠의 사용을 허가한다는 정보를 포함하는 증명서를 이용하여 서비스 제공 장치에게 상기 컨텐츠를 요청하는 요청부; 및

상기 서비스 제공 장치로부터 제공되는 상기 컨텐츠를 재생하는 재생부를 포함하는, 원격 디바이스.

【청구항 25】

제 24항에 있어서,

상기 증명서는 상기 메인 디바이스에 대한 정보와 상기 원격 디바이스에 대한 정보 중 적어도 하나를 포함하는, 원격 디바이스.

【청구항 26】

제 25항에 있어서,

상기 메인 디바이스에 대한 정보는 상기 메인 디바이스의 식별자와 공개키 중 적어도 하나를 포함하고, 상기 원격 디바이스에 대한 정보는 상기 원격 디바이

스의 식별자와 공개키 중 적어도 하나를 포함하는, 원격 디바이스.

【청구항 27】

제 24항에 있어서,

상기 증명서는 상기 컨텐츠에 대한 사용 한도 정보를 포함하는, 원격 디바이스.

【청구항 28】

제 24항에 있어서,

상기 증명서는 상기 메인 디바이스의 개인키로 암호화되어 있는, 원격 디바이스.

【청구항 29】

제 24항에 있어서,

상기 서비스 제공 장치로부터 제공 받는 컨텐츠는 상기 컨텐츠의 재생 한도를 제한하는 임계값을 포함하는, 원격 디바이스.

【청구항 30】

제 24항에 있어서,

상기 서비스 제공 장치로부터 제공 받는 컨텐츠는 상기 원격 디바이스와 상기 서비스 제공 장치에 의해 공유된 정보를 통해 암호화된, 원격 디바이스.

【청구항 31】

제 30항에 있어서,

상기 공유된 정보는 상기 원격 디바이스의 식별자와 상기 원격 디바이스의 공개키 중 적어도 하나를 포함하는, 원격 디바이스.

【청구항 32】

컨텐츠에 대한 재생 권한을 갖는 메인 디바이스로서,

상기 컨텐츠의 사용을 허가한다는 정보를 포함하는 증명서 생성하는 증명서 생성부;

상기 생성된 증명서를 원격 디바이스에게 전송하는 통신부;

상기 원격 디바이스에게 상기 컨텐츠를 제공하려는 서비스 제공 장치로부터 상기 컨텐츠를 재생시킬 수 있는 권리 객체의 상태 정보를 갱신하도록 요청 받은 경우, 상기 상태 정보를 갱신하는 제어부를 포함하는, 메인 디바이스.

【청구항 33】

제 32항에 있어서,

상기 증명서를 이용하여 재생할 수 있는 컨텐츠의 목록을 생성하는 컨텐츠 목록 생성부를 더 포함하고,

상기 생성된 목록은 상기 통신부에 의하여 상기 원격 디바이스에게 전송되는, 원격 디바이스.

【청구항 34】

제 32항에 있어서,

상기 상태 정보가 갱신되었음을 나타내는 정보를 포함하고 상기 서비스 제공

장치에게 전송될 응답 패킷을 생성하는 응답 패킷 생성부를 더 포함하는, 원격 디바이스.

【청구항 35】

제 34항에 있어서,

상기 응답 패킷은 상기 제어부에 의해 상기 메인 디바이스의 개인키로 암호화된, 메인 디바이스.

【청구항 36】

제 32항에 있어서,

상기 상태 정보 갱신부는 상기 원격 디바이스에게 전송된 상기 증명서가 상기 서비스 제공 장치로부터 수신된 경우, 상기 상태 정보를 갱신하는, 원격 디바이스.

【청구항 37】

제 32항에 있어서,

상기 증명서는 상기 메인 디바이스의 개인키로 암호화된, 메인 디바이스.

【청구항 38】

제 32항에 있어서,

상기 증명서는 상기 메인 디바이스에 대한 정보와 상기 원격 디바이스에 대한 정보 중 적어도 하나를 포함하는, 메인 디바이스.

【청구항 39】

제 32항에 있어서,

상기 증명서는 상기 컨텐츠에 대한 사용 한도 정보를 포함하는, 메인 디바이스.

【청구항 40】

디지털 저작권 관리를 위한 서비스 제공 장치로서,

원격 디바이스로부터 증명서 및 컨텐츠 전송 요청이 수신되는 경우, 상기 증명서가 메인 디바이스에 의해 발급되었는지의 여부를 검증하는 증명서 검증부; 및

상기 증명서가 상기 메인 디바이스에 의해 발급된 것일 경우, 상기 컨텐츠를 상기 원격 디바이스에게 제공하는 컨텐츠 제공부를 포함하는, 서비스 제공 장치.

【청구항 41】

제 40항에 있어서,

상기 메인 디바이스의 구매 이력을 검사하는 구매 이력 검사부를 더 포함하고,

상기 컨텐츠 제공부는 상기 메인 디바이스가 상기 컨텐츠 또는 상기 컨텐츠에 대응하는 권리 객체를 구매한 이력이 확인된 경우에 상기 컨텐츠를 상기 원격 디바이스에게 제공하는, 서비스 제공 장치.

【청구항 42】

제 40항에 있어서,

상기 메인 디바이스에게 상기 컨텐츠를 재생시킬 수 있는 권리 객체의 상태 정보를 갱신할 것을 요청하고, 상기 상태 정보가 갱신되었다는 정보를 포함하는 응답 패킷이 수신된 경우에 상기 응답 패킷을 통하여 상기 상태 정보가 갱신되었는지 검증하는 응답 패킷 검증부를 더 포함하고,

상기 컨텐츠 제공부는 상기 상태 정보가 갱신된 경우에 상기 컨텐츠를 상기 원격 디바이스에게 제공하는, 서비스 제공 장치.

【청구항 43】

제 40항에 있어서,

상기 원격 디바이스에게 전송되는 컨텐츠를 상기 서비스 제공 장치와 상기 원격 디바이스 간에 공유된 정보로 암호화하는 제어부를 더 포함하는, 서비스 제공 장치.

【청구항 44】

제 43항에 있어서,

상기 공유된 정보는 상기 원격 디바이스의 식별자와 상기 원격 디바이스의 공개키 중 적어도 하나를 포함하는, 서비스 제공 장치.

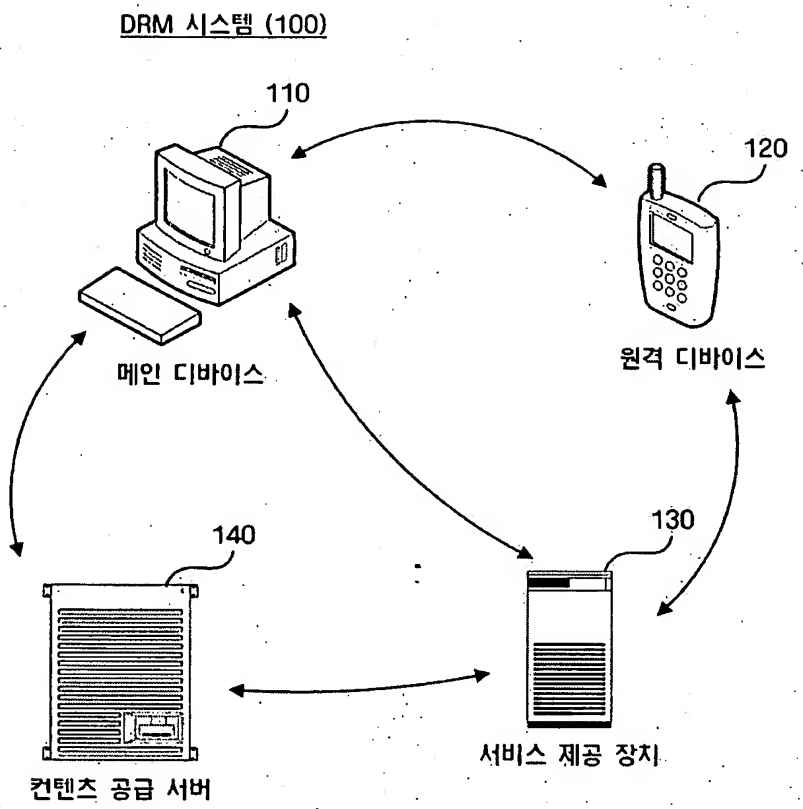
【청구항 45】

제 40항에 있어서,

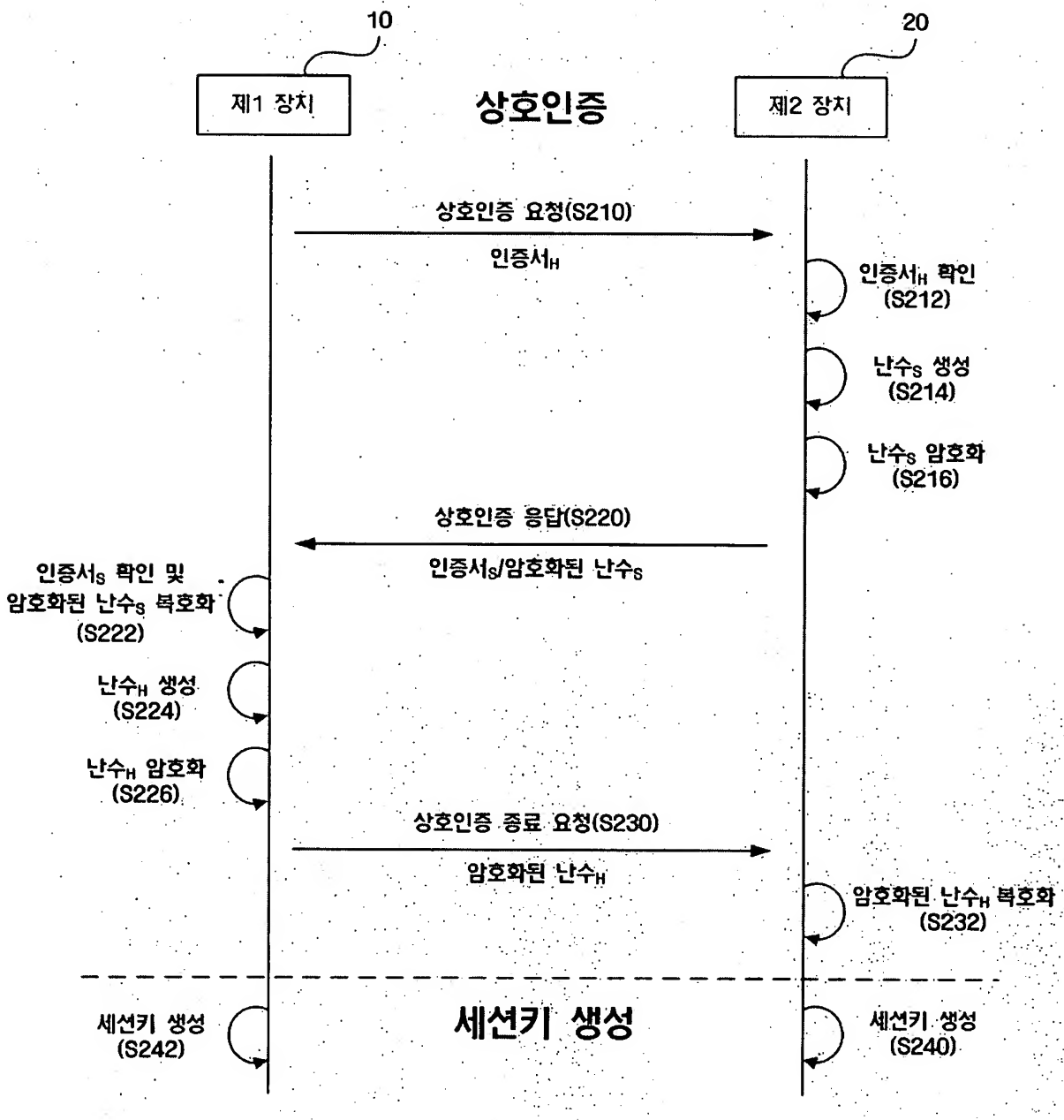
상기 제어부는 상기 컨텐츠의 재생 한도를 제한하는 임계값을 상기 원격 디바이스에 제공되는 컨텐츠에 포함시키는, 서비스 제공 장치.

【도면】

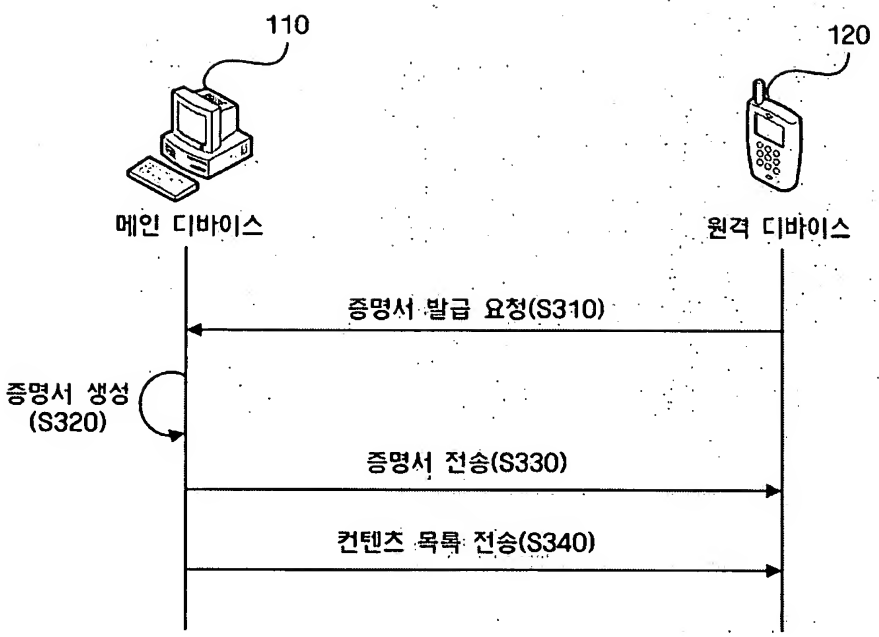
【도 1】



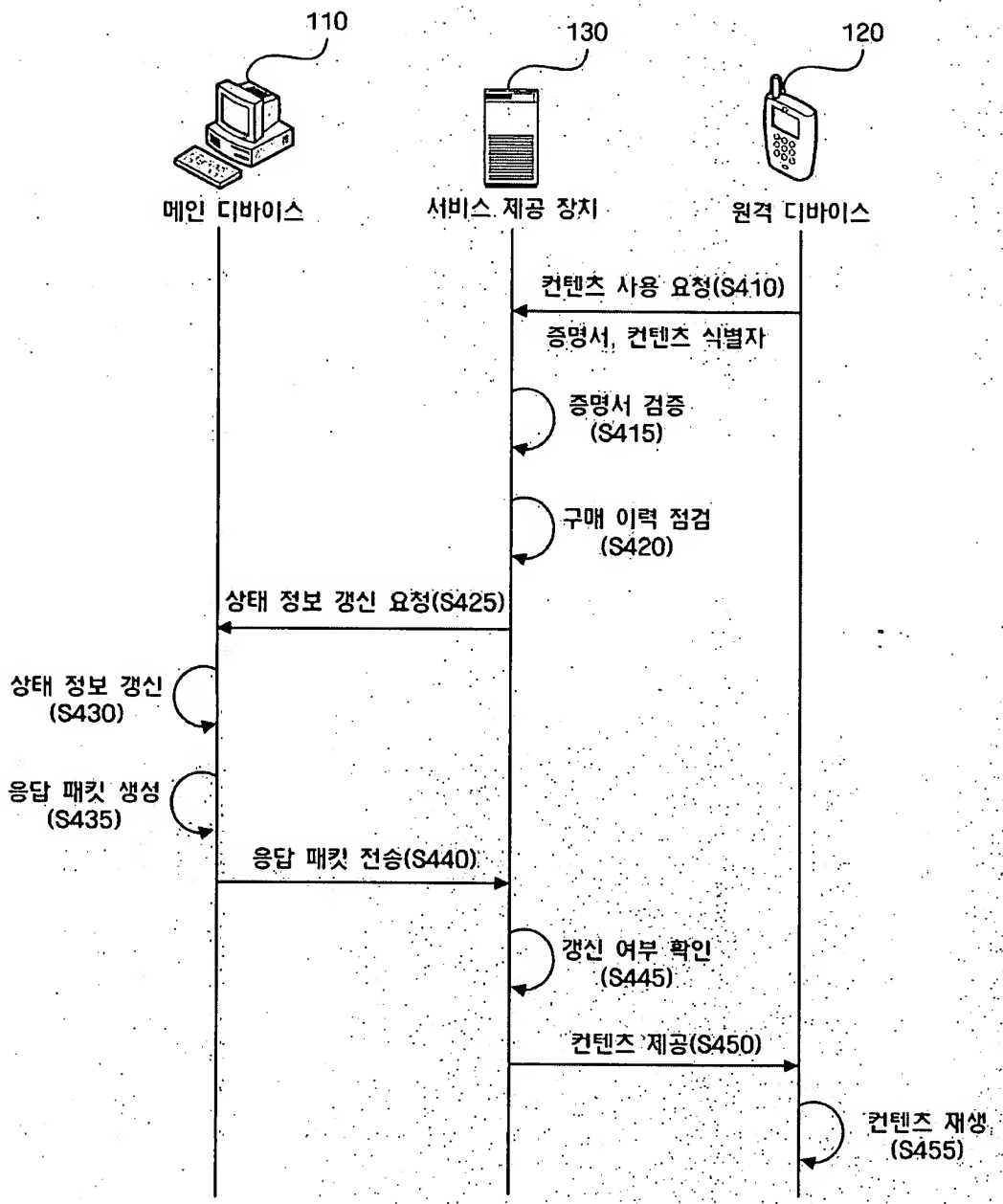
【도 2】


10
20
제1 장치
상호인증
제2 장치
상호인증 요청(S210)
인증서H
인증서H 확인 (S212)
난수S 생성 (S214)
난수S 암호화 (S216)
상호인증 응답(S220)
인증서S/암호화된 난수S
인증서S 확인 및 암호화된 난수S 복호화 (S222)
난수H 생성 (S224)
난수H 암호화 (S226)
상호인증 종료 요청(S230)
암호화된 난수H
암호화된 난수H 복호화 (S232)
세션키 생성
세션키 생성 (S242)
세션키 생성 (S240)

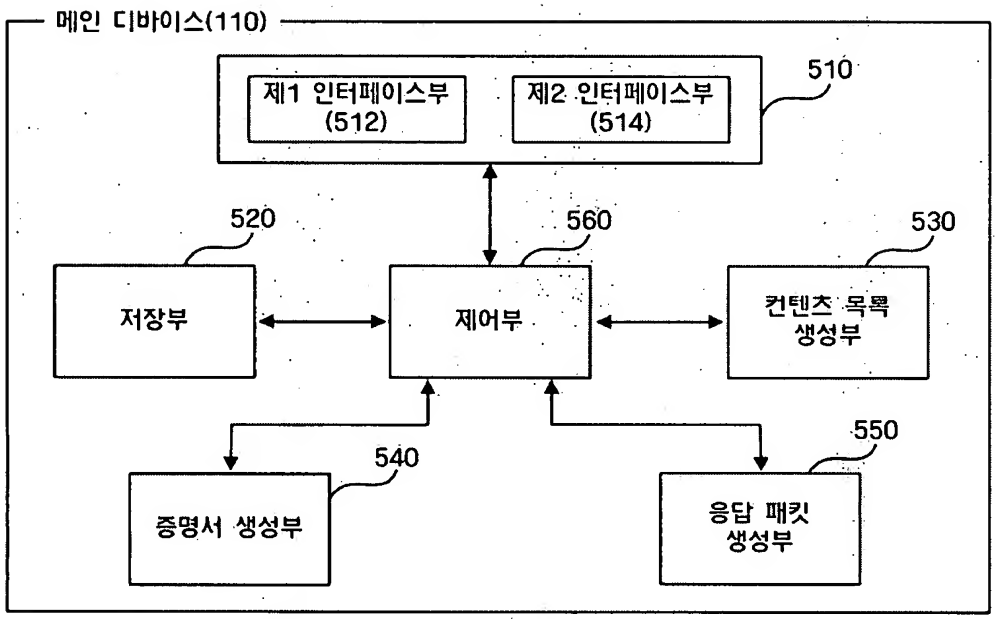
【도 3】


110
120
메인 디바이스
원격 디바이스
증명서 발급 요청(S310)
증명서 생성
(S320)
증명서 전송(S330)
컨텐츠 목록 전송(S340)

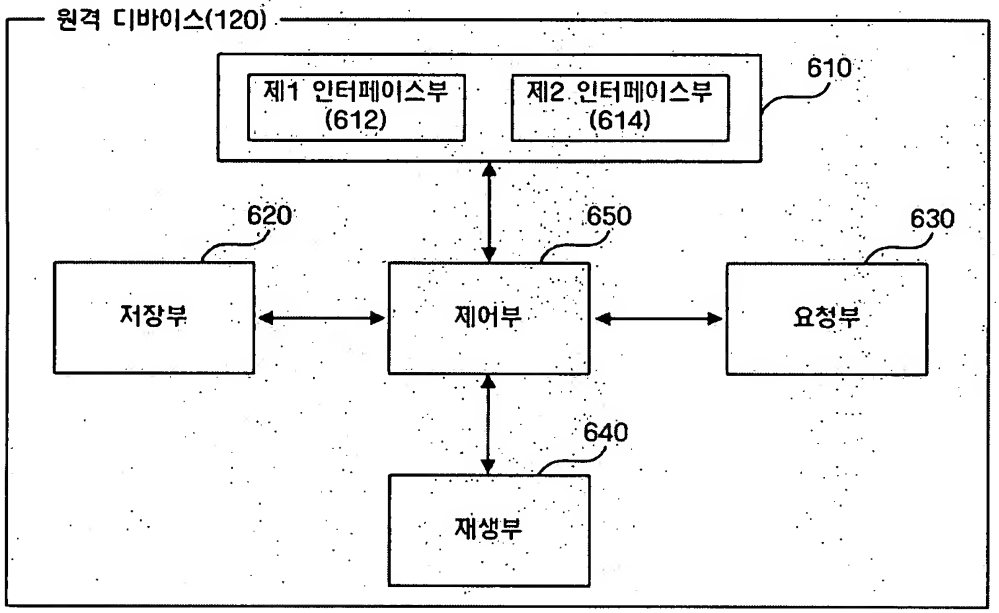
【도 4】


110
130
120
메인 디바이스
서비스 제공 장치
원격 디바이스
컨텐츠 사용 요청(S410)
증명서, 컨텐츠 식별자
증명서 검증
(S415)
구매 이력 점검
(S420)
상태 정보 갱신 요청(S425)
상태 정보 갱신
(S430)
응답 패킷 생성
(S435)
응답 패킷 전송(S440)
갱신 여부 확인
(S445)
컨텐츠 제공(S450)
컨텐츠 재생
(S455)

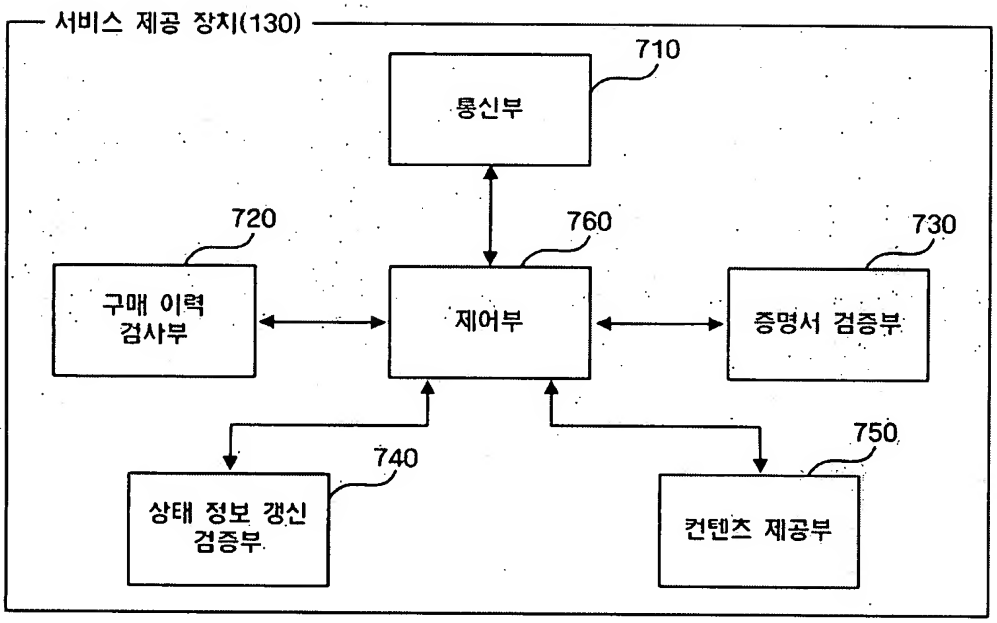
【도 5】


메인 디바이스(110)
제1 인터페이스부 (512)
제2 인터페이스부 (514)
510
520
560
530
저장부
제어부
컨텐츠 목록 생성부
550
540
증명서 생성부
응답 패킷 생성부

【도 6】


원격 디바이스(120)
제1 인터페이스부 (612)
제2 인터페이스부 (614)
610
620
650
630
저장부
제어부
요청부
640
재생부

【도 7】


서비스 제공 장치(130)
710
통신부
720
구매 이력 검사부
760
제어부
730
증명서 검증부
740
상태 정보 갱신 검증부
750
컨텐츠 제공부